AIR FORCE CYBERWORX REPORT 16-003:
A RESPONSIVE CYBER RISK ECOSYSTEM

MICHAEL V. CHIARAMONTE, Lt Col, USAF
Senior Designer & Facilitator

JEFFREY A. COLLINS, Col, USAF
Director, AF CyberWorx

DESIGN PROJECT CONDUCTED
11 AUG – 7 DEC 16

Produced with input from numerous units at Peterson AFB, Buckley AFB, and Schriever ABF. Designed by USAFA Cadets, Officers, and our valuable partners in Industry.

Air Force CyberWorx™
2354 Fairchild Dr, Ste 2N300
USAF Academy, CO 80840
AFCyberWorx@usafa.edu - @AFCyberWorx - (719) 333–4278

Introduction

CyberWorx is a dynamic organization partnering Airmen, industry, and academia to reimagine how technology might enrich and protect our nation, businesses, and lives. As a human-centric design center, we seek out unique ways to connect Air Force warfighters with current and future technology in meaningful ways. We look to transfer, license, and share promising prototypes, solutions, and knowledge with our partners to create value for both the warfighter and the economy as this is the best way toward operational advantage.

Design Thinking

Design thinking is a common sense, human-centric problem solving method embraced by industry leaders such as Apple and Google but often overlooked in the government sector. The CyberWorx design thinking process is a transdisciplinary method that breaks down silos of standard organizational structures. Organizations naturally form structures based on specializations to facilitate deep expertise, but these structures often impede creativity, collaboration, and knowledge sharing vital to innovation. CyberWorx deliberately reaches across specialties to bring diverse perspectives to a problem in a non-threatening environment. This evokes ideas that would otherwise be missed or stifled. The transdisciplinary design approach teases out meaningful solutions that are intuitive and desirable to Airmen.

> The CyberWorx design thinking approach deliberately breaks through the military's hierarchical and mission silos to find hard-hitting answers.

Air Force CyberWorx offers facilitated design thinking sessions that bring stakeholders, industry and academic experts together to develop solutions to hard problems. These sessions are tailored to best meet AF needs with differing lengths based on time sensitivity and CyberWorx capacity. One method, which maximizes the educational benefit to cadets and industry partners, is to offer a design course where the semester long design project is a challenge being worked for AF stakeholders. The goal of such a design project is to develop low fidelity prototypes that clearly convey the desired Airman experience and the technical and policy developments needed to bring that experience to fruition. These projects help refine the requirement

by seeking the right problem to solve and find meaningful solutions by exploring a wide range of possible answers to the design problem.

For the Responsive Cyber Risk Dashboard Design Project, CyberWorx brought together a design team of 25 participants from UASFA and Industry to explore how cyber risk to AF mission sets should be conveyed. The goal was to develop a concept to convey risk in a manner that is intuitive and while providing the information to support rapid mission assurance decisions at the basic, operational and strategic levels of war.

Figure 1: Cadet and industry designers outbrief a conceptual cyber risk ecosystem. The present-ation consSited of a hypothetical scenario and rough prototype demonstrations.

Participants

The design project brought industry expertise to cadets and active duty operators; those differing perspectives provided unique value distinct from military members and government civilians. The CyberWorx design thinking approach deliberately breaks through the military's hierarchical and mission silos to find hard-hitting answers. This project included a variety of expertise including cyber security professionals, economists, systems engineers, business managers, operations research analysts, and software developers. During the project the design team observed active duty, reserve, and air National Guard operations including, defensive cyber operations, DODIN operations, space operations, mobility operations, base defense operations, and fighter operations.

> Commanders need cyber-risk presentations that are mission-oriented, not IT-systems oriented

Design Problem

Create a platform for AF leaders to convey mission focused cyber risk relevant to their domain to support commander decisions at the strategic, operational, and tactical levels of war. Identify cyber domain related decisions critical to AF warfighter mission needs. Define risk presentation views that support commander decisions enabling multi-domain mission success.

Theme Discovery

The early stages of a design project and the design thinking methodology call for analyses of the users' work environment, their desires, and their dislikes to inform and revise the initial problem statement. As part of the design process, the participants spent time delving into the various facets of the challenge to ensure they understood the challenge and were working on solving the right problem. This included observing operations in the Air, Space and Cyber domains, interviews with commanders, operators, subject experts, and industry leaders. These observations, experiences and views provided an unparalleled view of the problem that could not be achieved within a homogeneous group.

Leveraging this unique group, we discovered underlying problems that hinder the conveyance of cyber risk information in a way easily accessible to non-cyber professionals. When considering how to overcome these issues the design team identified four key themes that were addressed:

- ***Mission Dependencies,***
- ***Communication***,
- ***Education***,
- ***Crowd Sourcing***

These themes formed the foundation of a proposed online eco-system that ingests data at the system and user level, and translates that to effects on inter-dependent missions. This ecosystem provides support aids to overcome communication and language differences to maximize the speed with which a user can consume risk information to make informed decisions.

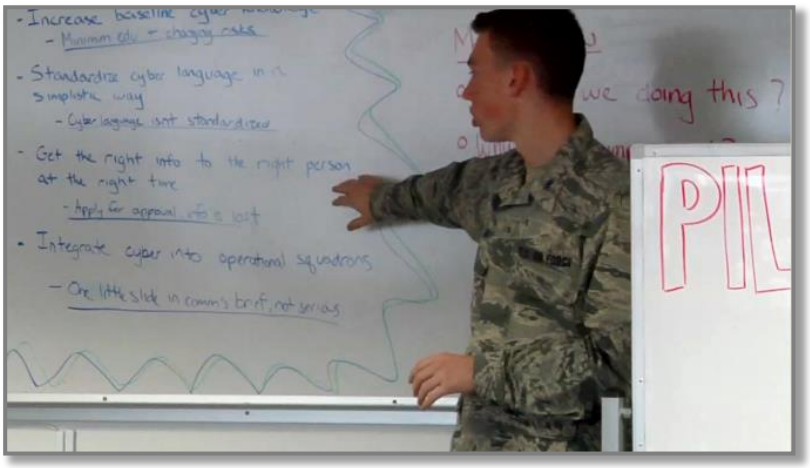


Figure 2: The design team briefs key insights and findings from inter-views, and observations of AF operations.

Design the Story to Convey the Experience

Progressing through the design process requires teams to analyze and organize information in a manner that communicates efficiently with stakeholders. This communication is aided by the development of user-

centered stories that are representative profiles and scenarios that humanize the design focus and test possible solutions.

To convey the power of the proposed ecosystem, we will follow a scenario that explores the mission dependencies between medical, flying and cyber operations. This story is a generalization to convey the use cases and user interactions of this new risk ecosystem and is not intended to be a summary of a real world event.

Dependency Mapping

Achieving mission assurance is not possible without understanding the linkages from systems and infrastructure to capabilities and missions. Functional Mission Analysis (FMA) is a disciplined way to tease out these linkages and integrate that metadata into our reporting systems and decisions. The AF has begun the FMA process at several bases to identify "key cyber terrain" to facilitate a workforce transition from focusing on providing IT services to focus on assuring Air Force missions.

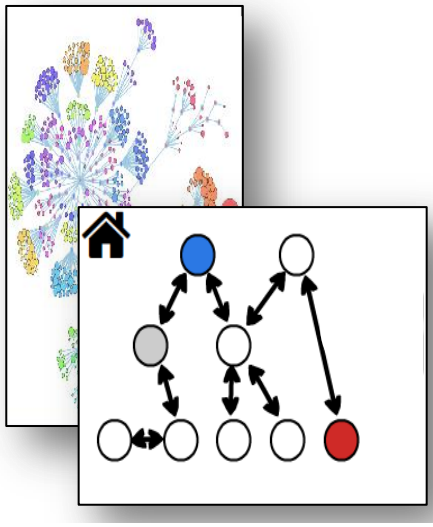


Figure 3: Mission dependencies (not system) displays can be drilled into for more detailed data. At a high level each mission bubble will convey the current risks to mission assurance. Views can be customized based on user preferences.

At 0730, Lt Col Howe, the 94th Fighter Squadron (FS) commander, arrives at work and logs into her cyber dashboard. Upon viewing the dashboard she sees there is a slight risk to her daily mission due to DODIN Ops mission degradation. Clicking on her unit, a mission risk dashboard shows her unit can expect slow internet connections that may cause slight delays in accessing MX information for the F-22. After a quick conversation with the Maintenance Squadron (MXS) commander, Lt Col Howe is confident her missions for the day will take off on time.

Reviewing the mission tasking for the day with his Director of Operations (DO) at 0800, Lt Col Howe sees that two pilots, Capt Hawking and 1st Lt Jones, are scheduled to be cleared for flying status by the 1st Medical Group (MDG) this morning at 0830 and then fly in the afternoon. Both Hawking and Jones got hurt playing intramural basketball last week.

Figure 4: Tailored information dissemination based on user and role mitigates info overload.

Halfway through the meeting, Lt Col Howe's cyber dashboard alerts her to a new notification that medical services are degraded due to an outage. The system lets her know the medical group may not be able to clear the pilots for flying directly, impacting two scheduled sorties.

Immediately Lt Col Howe begins engaging with the flight schedulers to determine alternative pilot-sortie assignments and with the 1st MDG to determine if her personnel can get cleared.

Communication and Education

During this project the design team visited three Colorado bases. Themes emerged that highlighted significant problems on how we communicate about cyberspace across specialties and within the cyber community. First and foremost, the language used was inconsistent from unit to unit and did not align with traditional operations vocabulary. Second, the cyber operations units tended to over-communicate, providing more information than relevant and making it hard for non-cyber decision makers to consume, understand, and act on the information in a timely fashion. Possible methods of communication suffered from a lack of universal understanding of cyber.

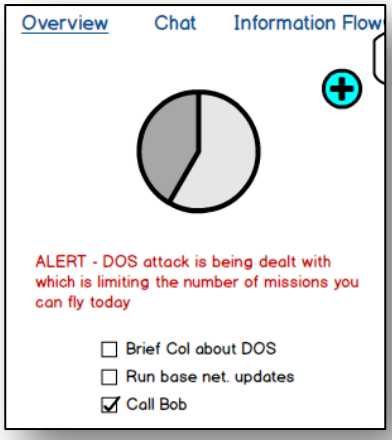


Figure 5: Real-time data for relevant risks are reported to a user's dashboard.

Finally, traditional Air and Space operators often left Cyber operators in the dark about planned missions and impacts of cyber systems on missions. There were no attempts to get on the same page and no effective means of doing so. The proposed cyber risk ecosystem addresses these issues by providing quick communications methods, information pushes, tailored delivery of information, and basic education.

When Lt Col Howe reported to her unit last year she logged into the cyber risk dashboard for the first time. Upon logging in her profile with her unit, job and contact information customized notification and data to ensure Lt Col Howe only receives information that impacts her. Since she was a DO at another unit the system remembers the presentation formats she likes best. These formats can include tree and graphs layouts for FMA dependencies as well as Gantt and pie charts for problem resolutions. This semi-customized presentation ensures the best consumption of data by the user.

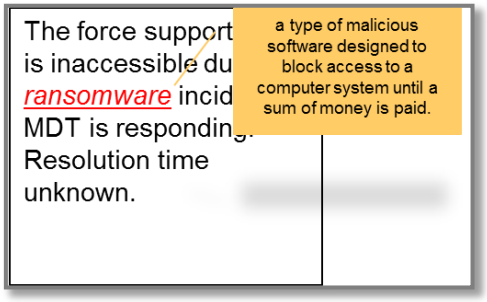


Figure 6: A word bank highlights all specialized terms to provide users with instant clarification on what they mean. This reduces miscommunications due to specialized AFSC language differences.

This morning when Lt Col Howe received the notification concerning medical system outages, the systems called CHCS and AHLTA were cited as the cause of the mission impacts. Since these are specific specialized terms, Lt Col Howe noticed they were highlighted on the screen in a similar way to how spell checkers underline questionable words. To learn more she positioned her mouse over the highlighted word and a pop-up appeared that draws on an official word bank to clarify what the terms mean. In this case, his popup reads "Currently all appointments are booked in the Composite Health Care System (CHCS), except for Walk-Ins and Telephone Consults, which can now be booked in via the electronic medical records system, Armed Forces Health Longitudinal Technology Application (AHLTA)." This info clarifies the cause of the outage and provides more insight into what is happening; as a result Lt Col Howe is more prepared to have a conversation with the 1st Medical Group.

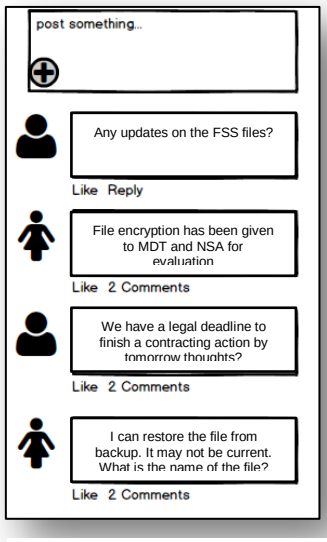


Figure 7: Chat and forums provide push button simplicity for issue stakeholders to interact and share.

> Cyber operators often over-communicate about systems, making life hard for mission decision-makers

For each ongoing incident and for general inquiries, the proposed ecosystem integrates modern chat, micro-blogging, and group forum capabilities to allow immediate and asynchronous sharing of events, impacts and other issues. This capability links the MDT and AF mission stakeholders in one click. Users don't need to search for phone numbers, wait on voice menus or deal with searching the GAL for the appropriate POCs. Responses to posts and chats can be made public to all users of the dashboard, certain groups of users, or private between two individuals as appropriate. Furthermore these activities allow for continuity of communications between user groups and are more quickly found and followed via the dashboard vice group emails (mixed with all other emails) in the standard email client.

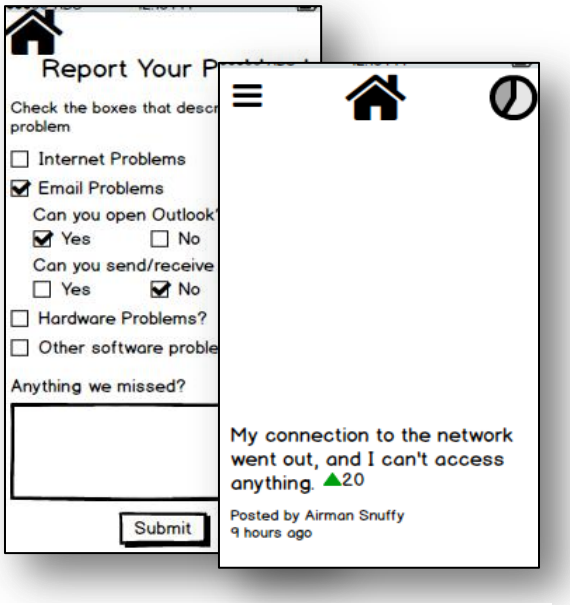


Figure 8: User reported issues inform FMA and provide visibility into the accessibility of capabilities rather than the status of individual IT systems.

Crowd Sourcing

Soliciting information from the masses is a crtical way to get rapid feedback on systems, capabilities, and missions. In the cyber risk ecosystem, crowd-sourced data facilitates mission assurance by identifying issues quickly, providing guidance toward systems fixes to restore systems, and providing guidance on alternative solutions to keep missions resilient. At 0800, A1C Jacobs arrives at work, logs in and tries to open AHLTA and the CHCS only to find his access is down.

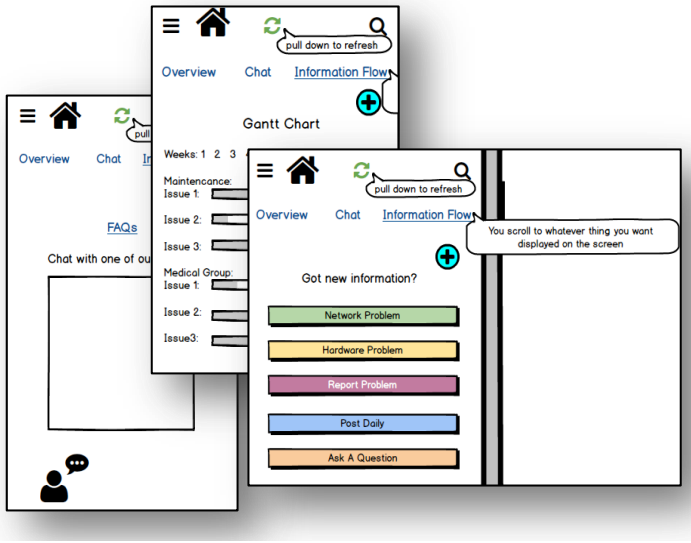


Figure 9: Collected user information from across the AF informs actions and controls expectations.

Quickly chatting with coworkers it appears no one can access the systems. To find a quick resolution he opens his dashboard and reports the loss of access to both systems and reviews open network issues for his installation. Based on his report the local Mission Defense Team (MDT) recieves a notification and the dependency mapping is updated to show medical services as degraded (lacking the ability to make new appointments and verify medical statuses such as PRP, flying etc). This update sends a notification to the user dashboards whose missions may be affected, alerting them of the impact and expected duration.

After receiving the notification, the MDT reviews crowd-sourced data provided by MDTs and PMOs. This data includes troubleshooting and resolution recommendations from previous incidents at their installation as well as AF-wide incidents involving loss of access between CHCS and AHLTA. By observing this data they recognize two issues involving routing and crypto that are common across AF AHLTA and CHCS problems. This information allows the MDT to quickly narrow the resolution down to a routing issue and tasks the DODIN operators to institute a fix. With a fix action planned, the MDT updated the expected resolution time on the dashboard. Since the routing issue is related to the general network degradation where the base rerouted traffic off the primary circuit, the MDT updates the FMA matrix for the installation to reflect the new data discovered about the mission dependencies. Finally the MDT upvotes the useful crowd-sourced data that expedited their solution discovery to make it more visible to other MDTs.

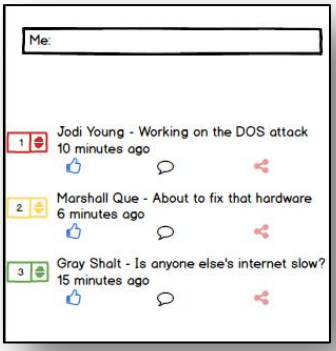


Figure 10: Up-voting and down-voting filters good and bad solutions to cyber problems. Likewise it provides work arounds to keep missions flowing in the event of cyber outages.

While the MDT is working, providers at the 1st MDG review their crowd-sourced mission alternatives and notice multiple bases have taken to providing a written appointment record for key appointments to minimize the impact to operations when CHCS and AHLTA are inoperable. Reviewing the information, the providers quickly benchmark an approved alternate way ahead to ensure critcal appointments and walk-ins can proceed. As a result, when Capt Hawking and 1Lt Jones walk in to be cleared for flying at 0830 the flight clinic is prepared to see them and both officers are cleared to fly.

Summary of Benefits

The proposal presented in this report includes elements to overcome limitations in the AF that hinder the ability to convey, understand and make decisions about cyber risks. These issues were observed in the field across mission sets and operating domains. They were further articulated to our design student by operators, leaders and stakeholders. It is important to note many of these reccomendations are extensible to other problem domains (outside of cyber) and may represent a desired solution across many specialties.

Recommendations

Air Force CyberWorx recommends a phased approach toward implementing all aspects of this proposal as described below.

Functional Mission Analysis

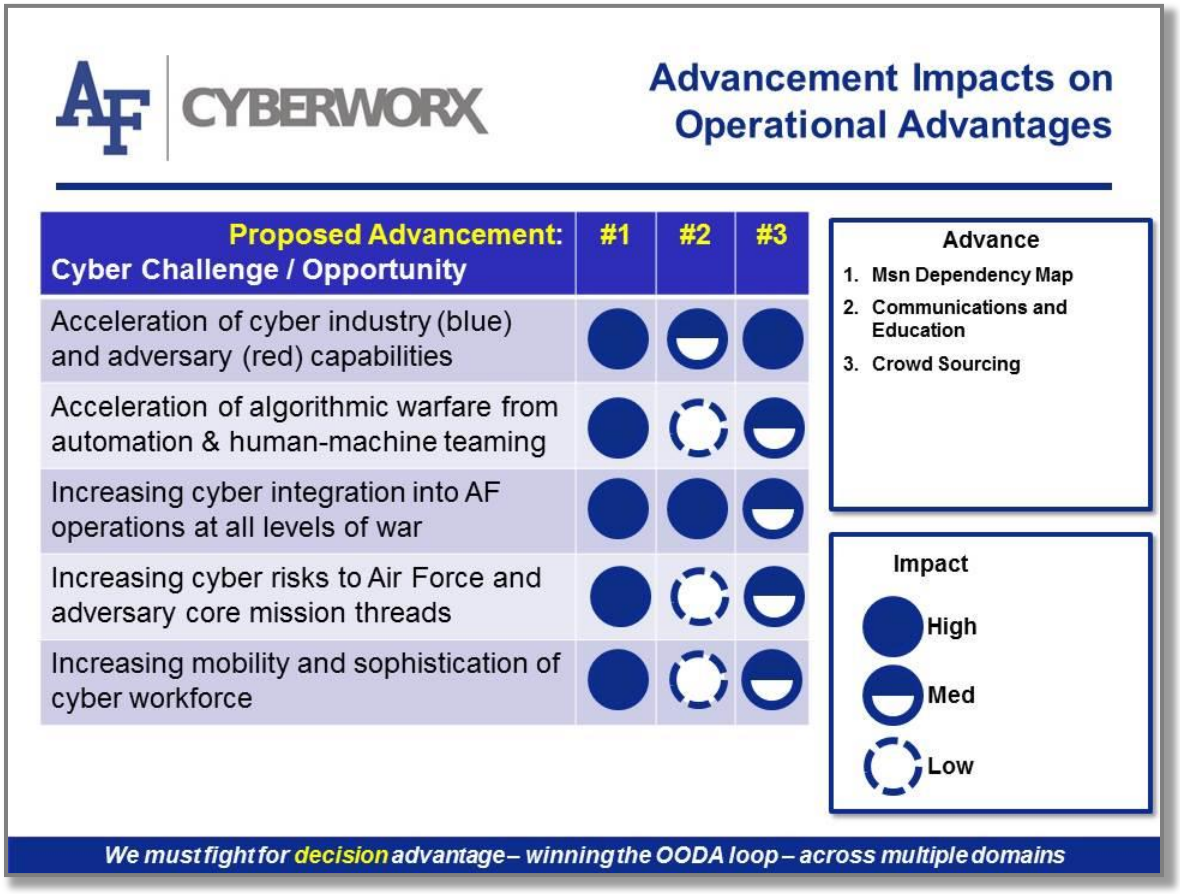
1. Accelerate the move toward functional mission analysis
    a. Create an AF standard process with an underlying data model.
    b. Create template FMA matrices for general mission types (e.g. medical, F-16, MX etc…). These templates should be crowd-sourced from the pathfinder cyber squadron units.

Platform Prototyping toward Development

1. AF CyberWorx will leverage rapid acquisition processes (e.g. existing Private Intermediary or DIUx Commercial Solutions Openings process) to create viable proofs of concept (POC) for experimentation, integrating existing commercial and open source platforms (e.g., chat and social features) when possible
2. Field and evaluate POC(s) at the cyber proving ground and pathfinder bases.
3. Move the most promising POC to Pathfinder Cyber Unit for operational assessments.
4. Work with leading vendor to iterate development toward a dual use COTS solution to ensure a sustainable maintenance tail.

Two Slide Summary: Ops Advantages + The Fast Track

The CyberWorx "two slide" summary section is designed to help in consideration of the recommendations in this report by weighing the operational improvements proposed against the current cyber challenges and opportunities we face as an Air Force.



In deciding what to do, the decision to do nothing is a decision and brings its own risks. Thus, the "fast track" slide spells out a recommended set of actions to take at minimum to put the Air Force on a path of discovery in overcoming the challenges that drove this design project.

AF | CYBERWORX

A fast track ahead

- Set up a sprint to formalize an AF FMA process and data model

- Test OTA and other faster contracting options to mature the Responsive Cyber Risk Dashboard to a prototype that can be evaluated as a proof of concept.
  - Informs rapid AQ processes and further explores the presented concept's feasibility, desirability and viability w/o a large investment.
- Engage with pilot unit(s) to get more detailed feedback on a proof of concept.

Integrity - Service - Excellence 2

CYBERWORX™